A B S T R A C T

A METHOD OF PROTECTING A CRYPTOGRAPHIC ALGORITHM

5   The method of protecting an algorithm that can be decomposed into the form of initial polynomials (P_i) of at least two variables and of degree not less than two, comprises the steps of making combined polynomials (Q_k) each obtained from at least two initial polynomials (P_i,

10   P_{i+1}), and of storing the combined polynomials (Q_k) in the form of a configuration file in a memory (3) associated with a processor unit (4).

15

20

25

30